Boston bombings raise questions for FirstNet

Urgent Communications *View from the Top* By Andrew Seybold April 22, 2013

The bombings during the Boston Marathon were a terrible tragedy, and the news media got a lot of things wrong in the first few hours after the blasts. One report, later retracted by the *Boston Globe*, was that the federal government had ordered all commercial networks to be shut down. No one knew if the bombs had been set off via cell phones, which is one of many ways they could have been detonated. The idea was that the networks were shut down was based on a fear that there could be more bombs, and the networks could be used to detonate them.

The real story was that the networks were not ordered to shut down, but they were so overcrowded that many call requests could not be put through. So many people being denied access to the networks led to the assumption that they had been shut down.

Even so, the fact that the networks were overloaded—as they are in times of major incidents—should be of concern to FirstNet. Because FirstNet is exploring the possibility of sharing the Nationwide Public Safety Broadband Network (NPSBN) with commercial operators, which will in turn make use of excess capacity on the network, the following questions need to be considered in the final network design. These questions are applicable during commercial-network overload, as well as when—and if—commercial networks are ever ordered to shut down.

1) If the commercial networks were to be shut down or become overcrowded, and the network operators had a sharing agreement to use the FirstNet network, would all of the users on the commercial networks be shifted over to FirstNet, causing increased traffic and congestion on the NPSBN when it is needed most by the first responders?

2) If commercial users had access to FirstNet and the commercial networks were shut down, does this also mean that the NPSBN would have to shut down, because a commercial device on this network would also be capable of detonating a bomb by remote control?

3) What—if any—safeguards will be built into the sharing agreements between FirstNet and the commercial network operators, and how will the load between FirstNet first responders and commercial users be monitored and managed? Will it be possible to shut down access to the NPSBN for secondary users (commercial users) when the commercial networks are shut down

or are overloaded?

The FirstNet system design is based on public safety having pre-emptive access to the network. In theory, pre-emption would occur in two phases. The first would be to limit the bandwidth and capacity available to non-first-responder users during incidents. The second would be 'ruthless pre-emption,' in which a first responder who accesses the NPSBN would be granted that access instantly, even if it meant terminating a commercial (secondary) user's connection.

This sounds great in theory, but in today's real world, any type of true pre-emption might not be possible. One of the committees I serve on is made up of some of the brightest LTE engineers in the business. They have participated in the standards body work for LTE, designed LTE systems, worked with LTE systems, and have more knowledge and hands-on LTE experience than any other group I have worked with or talked with. When I raised the following issues, they dug into them, and their top-line answers are shown after the statements.

Assertion 1:If the signaling channel is overloaded, then a User (UE) with maximum priority and pre-emptive rights may not be able to access the network.

Top-Line Answer:This is essentially a true statement, especially in a network that is shared with commercial users.

Assertion 2: LTE provides a way around this problem (as stated in Assertion #1) that can be implemented to ensure full priority access when needed.

Top-Line Answer: Mitigation tools exist in the 3GPP standards, but due to a wide range of potential scenarios and causes, to characterize this as "solved" would be an oversimplification.

There is much more to the response from this group that I will publish soon in my *Public Safety Advocate*
e-newsletter, but the reason for the response is based on the following overlying characteristics of LTE (or any cellular-like network):

1) In order to make a call (or get onto the network), the device must send a request for access to the network. The network then verifies that this unit is permitted access and attaches the device to the network.

2) The signaling channel input is located at each cell site, and it sends the request to the network. If the number of requests for service exceeds the capacity on the signaling channel, some of the requests will not be processed.

If the request for service or pre-emptive service is not delivered to the cell site and transmitted to the network, the network has no way of knowing the request was even made. Further, if the requests overload a number of cell sites, they may not travel from the cell site to the network for processing. In other words, if the LTE signaling channel (RACH) is congested, the level of priority makes no difference. If the cell site does not receive the request for service, it cannot be processed. So in reality, there is no true pre-emption in LTE today.

Note: One of the arguments we used with Congress to have the D Block allocated to Public Safety was the fact that pre-emptive access on commercial networks was neither practical nor feasible to accomplish. The earthquake centered in Virginia and the following hurricane proved our point, because—while the commercial networks remained operational—there were many instances when access was totally blocked because the signaling channels were overloaded.

The bottom line is that implementing the public-safety LTE system will be a real challenge. I am sure the FirstNet is up to it, but the solution will need to be carefully focused on the needs of public safety during incidents when access to the NPSBN will be critical for the public-safety community.

Link to Article

Link to Urgent Communications News Articles